TODO: How to list users and service accounts? How to list those privikliges? What is ABAC and RBAC?

This checklist maps to the file "Attacking Kubernetes".

External Pentest

- Check open ports
  - 443/tcp - Kubernetes API server
  - 2379/tcp - Etcd
  - 2380/tcp - Etcd
  - 6666/tcp - Etcd
  - 4194/tcp - cAdvisor - Container Metrics
  - 6443/tcp - Kubernetes API server
  - 8443/tcp - Minikube API server
  - 8080/tcp - Kubernetes API server
  - 10250/tcp - Kubelet - HTTPS API with full node access
  - 10255/tcp - Kubelet - Unauthenticated readonly. Pods/runnings pods/nodes
  - 10256/tcp - Kube-proxy - Kube proxy health check server
  - 9099/tcp - Calico Felix - Health check server for Calico
  - 6782-4/tcp - Weave
  - 44134/tcp - Tiller
  - 44135/tcp - Tiller
  - 30000-32767/TCP - Nodeport
- [ ] Check if API-server is exposed externally
- [ ] Check kubelet port 10255 (read only) for Information disclosure

Internal Pentest

Basic tests

- [ ] Check for anonymous access to `kube-apiserver`
- [ ] Check for anonymous access to etcd
- [ ] Check if kubelet port 10250 is accessible unauthenticated
- [ ] Check if kubelet port 10255 (read only) for Information disclosure
- [ ] Check for Service account secret / token
- [ ] Check for CVE-2018–1002105
- [ ] Check för usage of Helm
- [ ] HostPath - Mount Worker node root to pod
- [ ] Check if running Kubelet on master node
- [ ] Check for Docker-in-Docker
- [ ] Check for HostPid allow
- [ ] Check which services are exposed
- [ ] Check which versions kubernetes components are running

Authorization / Privilige escalation

- [ ] Check for interesting user and service account rights
- [ ] Check for CVE: CVE-2018-18264 Privilege Escalation
- [ ] Create Pod in Kube-system namespace and automount service account
- [ ] Deploy Pods using Create/update deployment, Daemonsets, statefulsets, ReplicationsControllers, Replicasets, Jobs, Cronjobs
- [ ] Privilege to use Pods/exec
- [ ] Privilege to Get/Patch rolebindings
- [ ] Check for impersonation privileges
- [ ] Check if RBAC is used

Security Audit

- [ ] Check if PodSecurityPolicy is supported
- [ ] Check if PodSecurityPolicy is used
- [ ] Static analysis of YAML files
- [ ] Check that pods are running as non-root users
- [ ] Check the usage of network policies